Indiana
Office of Technology
www.IN.gov/iot

MEMO

Re: Information Systems Inventory Update
To: All Information Systems Owners
Date: December 8, 2006

Thank you for recently updating the Information Systems Inventory (ISI) with current data about your application(s). As a recipient of this e-mail, you are recognized as an owner of systems containing personal information and have the important responsibility of assuring its appropriate defense. The following points require consideration as you execute your role as protector of personal information:

1. **Thoroughly understand how your information is used and where it resides**. Storing sensitive information on secure networked servers is the preferred practice. Personal information should only be stored on local desktop or laptop drives when absolutely necessary (not merely convenient). Know that sometimes users will move information from your application to spreadsheets and/or personal databases that are more familiar. Though this can be productive, it also exposes the personal information to increased risk. Prohibit such practices without your direct authorization (such authorization may include additional protective measures). Develop data use policies for your system, train users on system security, implement mechanisms to audit compliance and discipline violators.

2. **Know who is using the information**. Give access to information based on the role of the individual. Each role should have standardized access; that access should be the minimum required to perform their duties (avoid creating special or super users). Ensure that appropriate separation of duties and checks and balances are in place to limit the threat of misuse by single individuals. Perform appropriate background checks for users of personal information. Terminated staff should have rights to your system(s) removed immediately.

3. **Conduct risk assessments**. Know the threats to your system and the measures needed to mitigate risk. Understanding risks aids not only in protecting your system as it is, but also planning for future modifications. Talk regularly with your technical support team. Have them explain the safeguarding procedures in place and the opportunities for improving safety in the future.

4. **Incident planning**. Understand the actions you will take if your system protections fail resulting in the compromise of personal information. There are laws driving the proper and timely notification to parties potentially impacted. If the system includes personal social security numbers, be aware of the laws regarding prohibited disclosure and notification requirements under IC 4-1-10 (http://www.ai.org/legislative/ic/code/title4/ar1/ch10.html) and 4-1-11 (http://www.ai.org/legislative/ic/code/title4/ar1/ch11.html) and 10 IAC 5 (http://www.in.gov/legislative/iac/T00100/A00050.PDF).

This is not a comprehensive list but rather a good start toward protecting personal information. System ownership is a tough job with many time consuming duties. None, however, are more important than caring for your system's sensitive data.

Thank you again for updating the ISI. If you have questions or if I can provide assistance, please let me know.

Tad Stahl, CISO
Office of Technology